Are schools the safe space to err and explore?

Growing digitisation of schools prompts concerns over the ability of students (and parents) to develop informed decisions towards how, why, when and who uses school data. As technologies increasingly make record of students' every move, Velislava Hillman asks whether constant monitoring, micromanagement and data collection of students guarantee a safe environment for them to err without future negative consequences. [Header image credit: B. Flickinger, CC BY 2.0]

School is considered a safe space where children go to learn, to discover new things, to make friendships. But as we have seen in other seemingly safe spaces – from church and aid agencies, to scouts and sports clubs – children can be at risk of harm. This is not to slander schools, reject education technologies (edutech) or data collection. And to be clear, making mistakes refers directly or indirectly to learning (e.g. forgetting to study for a test, getting tasks or assignments wrong, even feeling sad or tired or simply not interested in a subject), not harming self or others. Additionally – and importantly – the freedom to make mistakes and experiment are integral to learning. But can constant monitoring and micromanagement of students' performance through algorithm-based technologies, score dashboards, and skill meters diminish basic freedoms of expression and self-efficacy?

Edutech tools: opportunities and challenges

The learning opportunities edutech tools provide are many. They help children with disabilities; provide global reach; tailor learning; enable collaboration and creativity. There are also positive aspects of school data generated from edutech: it can elicit useful information and improve work; advance education theory; leverage resources. However, as more tools infiltrate school processes – from applications that generate classroom surveys (what are children's political views?), monitor student-generated content (did anyone type 'kill'?) and control behaviour – the 'right to remain silent' may transpire as the best option for students under constant surveillance. The greater implications of collecting fine-grained data over a long time lies in its permanence, impact and reach. As some authors argue, 'datavaillance' in schools infringes upon children's rights. While laws such as FERPA, COPPA (for the US) and GDPR (for the EU) protect how children's data is handled, many providers lack transparency and consistent privacy and security practices.

What school data?

A school district typically uses agreed-upon data standards that organise data into hundreds of elements. Each element contains more granular data such as student names, address, gender, race, grades, teacher observations, accidents and more. A school may use more than 100 edutech products and services, usually supplied by for-profit companies. There are tools supporting teacher work; applications for grading and attendance, lesson planning, behaviour monitoring. There is incoming and outgoing data between schools and providers. With 'adaptive learning' tools infusing classrooms, detailed data is a prerequisite for the algorithms to tailor content with precision. Their use generates more data, which, if available, is likely to be incompatible with schools' data standards. But such data does not encompass everything there is to know or infer about a student. While legal frameworks address how children's digital data should be handled, alongside organisations, community and schools themselves who make great effort to guarantee student data privacy and security, data breaches continue to happen, providers' use of student data still lacks transparency and laws still have many flaws. Most of all, students (and parents) lack awareness of the complex data, the mechanisms of data collection, use and impact.

There are a number of measures that can enable such awareness and prioritise student data literacy and agency over their data. By sharing them, I invite teachers, edutech providers, and other researchers to join in with feedback and collaboration.

- **Create school data taxonomy** for the perusal of children and young people. Give visibility to students about what is collected about them, by whom and how it is used to evaluate them as individuals and as learners;
- **Enable transparency:** data will give students transparency about who does what, when and why with their data;
- **Prioritise student agency and participation** in school processes. It makes no sense for students to provide personal, emotional or academic feedback simply because every word can potentially convert into data and

Date originally posted: 2019-12-25

Permalink: https://blogs.lse.ac.uk/parenting4digitalfuture/2019/12/25/are-schools-the-safe-space-to-err-and-explore/

Blog homepage: https://blogs.lse.ac.uk/parenting4digitalfuture/

be processed by unknown algorithms that will infer about them with unknown consequences. Fine-grained data collection over a long period of time can destroy privacy, while various human agencies and authorities can obtain access to longitudinal data;
- **Engage different stakeholders:** educators, parents and edutech providers must join the discussion and ask whether it is safe to say that students can express their perspectives and feelings when their every word and action can amount to data that, decontextualised, can turn against their freedoms of self-expression;
- **Applied data literacy**: studies show that students have varying interpretations of data. Many find difficulties in connecting with data as a 'dossier'. A school dossier, however, can cover data from pre-primary school all the way to university and professional life. To enable data literacy students can start with their school data – understand how it is used and what it says and doesn't say about them as learners.

Protective mechanisms do not have to stifle development

Essentially, to keep up with data-centric technologies that infuse today's classrooms, the education domain must re-think protection strategically: build a number of data-protective layers that, at the same time, do not prevent leveraging from the use of insightful data and the advantages of educational technologies. Such layers should include, besides the hardware and software: legal and regulatory, enforced by technological design; learning and skill-building; and multi-stakeholder participation.

For educational applications to work they require a multitude of data elements about users. For example, SchoolCitySuite, an online assessment, management and analysis reporting system, collects IP addresses of users, metadata on user interaction with the application, test scores, student attendance, date of birth, gender, ethnicity, grade level, and more. A single platform with a simple, intutitive web interface (think iPhone's settings that give you in-app information about your daily use) can become an entry point to all educational stakeholders – edutech providers, education agencies and authorities, teachers, as well as students and parents. Such a platform can act as a checkpoint for incoming and outgoing data, whose design enforces concrete policies for data governance. When a third-party requests data use, the platform can enable a transparent process that also holds everyone accountable. Anyone can log in and see what student data SchoolCitySuite has accessed. Such technological mechanisms, built upon existing legal frameoworks, and now enforced by design, can automate data privacy protection while also enable comprehensive data sharing and communication across systems.

Most importantly, a common virtual ground can enable student agency and applied data literacy as its web interface gives an opportunity for students to interact with their data, understand and enquire about how various data they generate shapes their academic evaluation. This is the first step to learning to critically approach information, not simply accept it with complacency. Ultimately, this kind of self-evaluation is a form of reflection which is integral to learning.

Data ownership in baby steps

Today discussions surround a new Internet for all – a web space where users remain sole owners of their data. There is plenty to learn about the challenges that will come with such responsibility as owning and having to deal with one's own digital data. But as we begin to introduce children and young people to the digital footprint they leave behind while they enjoy the benefits of a hyper-networked world, we should equally bring their attention to the big data they generate as they go to school and ensure that they become well-informed individuals who do not fear making mistakes.

This article represents the views of the author, and not the position of the Parenting for a Digital Future blog, nor of the London School of Economics and Political Science.

Date originally posted: 2019-12-25

Permalink: https://blogs.lse.ac.uk/parenting4digitalfuture/2019/12/25/are-schools-the-safe-space-to-err-and-explore/

Blog homepage: https://blogs.lse.ac.uk/parenting4digitalfuture/